TOP SECRET

OUTLINE FOR RECAPITULATED "I" REPORTS

1. Summation
   a. General
   b. German Source information
   c. Japanese Source information

2. Cryptographic Security
   a. Codes
      (1) AACS PX Code
         (a) Latest information
         (b) Information lacking
         (c) Reconstruction
         (d) Method of attack
         (e) Conclusions

      (2) CD 0278 India Weather Cipher (Indicator--Rummy)
         (a) First indication
         (b) Progress made
         (c) Recovery

      (3) Chungking Army Air Force Weather Cipher
         (a) Change reported and listed
         (b) Again changed and new values given
         (c) Information requested

   b. Converter M-209
      (1) Foreign interest in Hagelin machine
         (a) Use indicates cryptanalytic development of country
         (b) C-36 picked up in Paris

      (2) Japanese interest in Hagelin--Tokyo's order for 6 machines

      (3) Japanese analysis of machine--report on construction and solution of Z Code
         (a) Amount of aid
         (b) Extent of solution

   c. Tactical Systems
      (1) New Guinea front line codes
         (a) Not interested in specific information from combat areas
         (b) Lack of intercept stations
         (c) Lack of personnel

      (2) Mention of "tactical code" messages by naval vessels

TOP SECRET

TOP SECRET

15-8-16

ARMY SERVICE FORCES

SIGNAL SECURITY AGENCY

WASHINGTON 25, D. C.

SECRET
By Authority of the
Chief Signal Officer
Initials Jwn Date 17 May 45

SPSIS-8A

17 May 1945

SUBJECT: Evidence of M-209 Solution in ZIP/SAC Reports

THRU: Director of Communications Research

TO: Commanding Officer
Signal Security Agency

1. As directed, ZIP/SAC/R. 13 A and ZIP/SAC/J.4 have been investigated thoroughly for information concerning the security of the M-209.

2. The references to the Converter found in the two ZIP/SAC reports and the parallel references in the three current "I" Reports are as follows:

ZIP/SAC	"I" REPORTS Report #.-
Page 4. Cipher leakage, etc.....	#2--March 44--Q 229 to Col. Connor HMOC/629--IS 21476--item (2)--page 24. #2--IS-20318--ZIP/SAC/W.18--item (1)--page 24. #3--11 Feb 45--IC-6-114--item (2)--page 5.
Graupe.....	#1--"G" P/W Interrogation--item (5)-- page 4.
Page 5. Excavations at NA 5 Paris....Material held out for special report.	
Pages 5 & 6. Memo iii Technical Data.....	#1--ER 38820-IR-7--item (2)--page 3.
Page 22. Exploitation of Signals sent in M-209 by German Sigint.....	#2--16 January--IS-20910--ZIP/SAC/W.19 of 7 August and 16 October--item (10)--page 26.

TOP SECRET

SPSIS-8A (17 May 1945)

Page 30. Japs helped on 209 by Finnish and German Crypt Bureau.....	#2--C-677--item (3)--page 24. #2--29 Sept--IS-14861--ZIP/SAC/W.17-- item (6)--page 25. #2--19 October--Horton to Collins--item (7)--page 25. #1--Headings on messages--items (b),(d),(f),(g),(h),(i)--page 2.
16th June Tokyo stated "The intermediate 6 letters of the indicator group".....	#2--C-677--item (3)--page 24.
Page 31. 31st July Investigation 209 and listed reconstructions in performance and indicator system.....	#1--C-641--item (1)(j)--page 3.
Page 41. Jap work on M-209.....	#1--C-648--item (1)(f)--page 3. #1--C-925--item (1)(e)--page 3. #2--September 44--Material Affecting U.S. Army Signals and Cipher Security--Notes for Col. Cook--item (4)--page 25. #2--DG 427-to SSA--item (8)--page 25.
28 September M-209 listed under Codes used between aircraft and their bases.....	#2--C-958-D--item (5)--page 25
25 February 5-letter code used instead of 3-letter code.....	#3--C-974-A,B--item (55)--page 3.

3. There were found only three references which had not been previously reported in "I" Reports. These references and their contents are quoted below. The documents from which the quoted references are taken were not available to us, although we have made a request concerning J-7110-A.

a. Page 5 of above-mentioned ZIP/SAC Report and British reference Z/DS 276, T 450/21, T 470/36, T 472/22 states:

TOP SECRET

SPSIS-8A (17 May 1945)

"M-209 Technical Data mentioned in Source.

"Section IV of Main Signals Recce Station, OKH, appears to deal particularly with M-209 traffic (Major Hentze signs). On 26th January this department passed back an enciphered M-209 text to O.C. Signals Recce 6 (Now in charge of part of the Army 'Y' Service on the Western Front).

"On the following day the same authority issued corrections to specified groups of another M-209 text which we had not seen.

"NA 7 Sigint HQ in Italy passed the following M-209 key back to the same Dept IV on 19th February; the report was highly proformalised and suggests a regular service of this nature:-

"AM 1 (M-209) Key for February 16th:- IIWW
Number of Lugs - 6, 12, 2, 4, 3, 1, of which 25 - 2 operate
Pin Settings -
1. A D E G H I L N Q T V W X
2. B F H I K Q T U V Z
3. A D G H J O Q R S T U V
4. C G H J K L P S U
5. A C E F G H K M P Q S
6. B E H I M N P

"On 23 February, Major Hentze was again responsible for ordering direct liaison between Sigint HQ's in Italy and the West (possibly because of the disorganisation of OKH Centralised control during their move away from Berlin) where technical reports on M-209 and M-209 decodes were concerned.

"It appears likely that Major Hentze who had previously worked with O.C. Signals Recce 5, formerly the only Cryptographic HQ for the Western Front, where it is known (see (i) and (ii) above) that considerable success with M-209 was achieved, has now been transferred to the Cryptographic Department of the Main Signals Recce Station responsible for research on the M-209 machine - and in this capacity he advises O.C. Signals Recce 6, now brought from the Eastern Front to help out NA 5 in the West."

TOP SECRET

b. Page 17 of ZIP/SAC 13 A and T 363/18, PROC 9342, PROC 9609, R 399 (C) 56 states:

"2. U.S. Sectors. (a) M-209 (German designation 'AM 1').

"References to the German exploitation of this cipher traffic have already been made on pages 5 - 6. Extracts from the few German Signit reports we have seen where specific mention of 'AM 1' (American Machine 1, the German designation for the M-209) have occurred, follow: (i) On 16th October 'As from 0200/18/10 pay attention to change in encoding with machine key of 7th August.' (ii) On 5th December a 'Y' report from ENAST 5 was seen the Traffic Analysis Section of which gave the following references to AM 1 '6th Army Group, 2460 kcs, three stations (JECU, JEAZ, JECT) AM1 signals - ground-attack aircraft success reports....one recce report about bridge near Breisach....7 U.S. Army (VI Corps) 4040 kcs, control and six stations (TKH, HAJ, RPA, RYQ, MYJ, MVI) - AM 1 signals - seven signals about M-209 recognised in area WEISSENBURG - BISCHWEILLER - STRASBURG. XV Corps, 2575 kcs, control and five stations (UXY, YDW, AUL, LWL, DTH) - AM 1 signals. 1 French Army. II Corps 2235 kcs, control and 2 stations (V--VEK) - AM 1 signals.

Aerodrome networks of XII TAC
3250 kcs, control K 60 AM 1 signals
3260 kcs, control 85A, Y98 - AM 1 signals.'"

c. Page 31 of above-mentioned ZIP/SAC Report and J-7110-A states:

"The following 'A' Intelligence from the 2nd Area Army, promulgated on the 8th December may possibly have derived from the reading of M-209 traffic:- 'The Allied GHQ which advanced to Leyte on and after 13th November, retreated to Biak on 7th December - it is not known whether this is Mac Arthur's or the 6th Army HQ.'"

4. The sum of the evidence in the ZIP/SAC reports including those previously incorporated in "I" Reports is as follows:

a. The Germans frequently broke messages sent in the M-209. Their analysts trained with the training traffic sent by our forces in England before D-Day. Only two types of compromises were exploited as the initial break into the system:

(1) Messages in depth led to cryptanalytic solutions. These solutions were completed in five to seven days and the information was not of tactical value, but was helpful in battle order and personality evaluations.

(2) Physical compromise of key lists enabled the enemy to read current traffic. In most cases, such compromises were a result of capture in tactical operations, although there is one mention of "a treasonable act." PWs expressed some amazement that compromises were not reported until harm had been done.

b. It was June of 1944 before the Japanese were sure of the M-209.

(1) Before that time they had considered it to be a code or a strip system. Espionage in Australia helped them to correct their misconception, but their knowledge was considerably increased by a capture, on Saipan, of two key lists which explained the indicator system. There has been little evidence, since that time, of Japanese success in reading the M-209.

(2) There are several mentions of a document, "The Report on the Construction and Solution of the Z Code," but no commendations are given by Tokyo, the common practice when field analysts achieve success. In view of this fact, it must be concluded that the solution was either effected in Tokyo or was obtained from the Germans.

(3) In regard to paragraph 3c, there is no evidence which would connect this "A" intelligence with the Converter M-209 except the fact that Second Army had a copy of the document mentioned.

M. G. JONES
Lt. Colonel, Signal Corps
Chief, Security Division